

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF OHIO  
WESTERN DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

v.

Case No. 1:21-cr-89  
JUDGE DOUGLAS R. COLE

JAMES A. BETHEL,

Defendant.

**OPINION AND ORDER**

This cause is currently before the Court on Defendant James Bethel's Motion to Suppress Evidence (Doc. 21), filed on October 20, 2021, in which Bethel challenges the government's search and seizure of his cell phone pursuant to a warrant issued regarding the premises at which he resides. The Court concludes that one principle controls the outcome here. Namely, as a general matter, when a search warrant validly issues against a premises, it is not suspect-specific, but rather extends to all items of the types the warrant specifies that are located at the premises, regardless of whether those items are owned (or used) by a particular suspect or not. An exception to that rule perhaps arises for personal property belonging to a guest who happens to be present at the premises when a search occurs—and who may have separately cognizable privacy interests. But that exception does not apply here. Accordingly, as more fully set forth below, the Court **DENIES** Bethel's Motion (Doc. 21).

## BACKGROUND

Bethel had the misfortune of sharing a residence with Nicholas Bonavita. (Mot., Doc. 21, #50). The Court refers to it as misfortune because, over the course of ten months from June 2020 through April 2021, the Federal Bureau of Investigation had been investigating Bonavita concerning potential distribution of child pornography. (*Id.*). This investigation involved, for example, obtaining records from Kik, an online file sharing service sometimes used to exchange child pornography, as well as tracking various IP addresses where agents believed that downloads of child pornography were occurring. (*Id.*). During this investigation, agents confirmed that the physical addresses corresponding to these IP addresses included Bonavita's workplace and, as particularly relevant here, what appeared to be his home address at 36 Sioux Court, in Batavia, Ohio. (*Id.*).

Based on their investigation, on April 21, 2021, agents sought and obtained a search warrant for Bonavita's residence. (*Id.* at #51). Bethel admits that the search warrant was supported by probable cause. Indeed, he concedes that there was "strong evidence that Mr. Bonavita had distributed child pornography." (*Id.* at #50).

The search warrant extended to "36 SIOUX CT., BATAVIA, OHIO 45103," which the warrant referred to as the "Premises." (Search Warrant, Doc. 21-1, Ex. A, #80). It authorized agents to search the Premises, including "all curtilage and vehicles parked on the subject Premises." (*Id.*). The warrant also specified the items to be searched and potentially seized at the Premises. As relevant here, this included all "[c]omputer(s), including cell phones" located at the Premises (*Id.*, Ex. B, #81).

On April 23, 2021, law enforcement officers executed the warrant. (Mot., Doc. 21, #49). Although it appears that the agents did not know it at the time (the record is not entirely clear on the extent of their knowledge), Bonavita did not live alone at that address. Rather, Bethel (age 43) and Bethel's parents also lived there. (*Id.* at #51). In any event, according to Bethel, the agents executed the warrant in "the very early morning hours, roused the residents from their sleep, and got everyone into vehicles outside the residence." (*Id.*). Particularly relevant to the instant Motion, during the search the agents found a cell phone in Bethel's room, sitting on a charger. (*Id.*). They then brought the cell phone to Bethel so he could call his girlfriend. (*Id.*). After that, they took the cell phone back from him, and conducted a manual search on it. (*Id.*).

The manual search led to the discovery of photographs stored on the cell phone depicting children engaging in sexual conduct. (Opp'n, Doc. 22, #95). Those photographs, along with other information gleaned from a further investigation that the officers undertook after discovering the photographs, form the basis for the charges in the Indictment in this matter.

On October 20, 2021, Bethel moved to suppress the evidence discovered on his cell phone, along with any "fruits of the poisonous tree." (*See* Doc. 21). His basic argument is that, while there may have been probable cause to search *Bonavita's* cell phone or computers on the Premises, there was not probable cause to search *Bethel's* cell phone, also located there. Thus, he claims that the search warrant, while valid as to the former, did not provide agents authority to search the latter. The government

opposed Bethel's Motion. (Doc. 22). The Court (the matter was assigned to a different judge at the time) held an evidentiary hearing on April 21, 2022. The only witness to testify was Keith Isaacs, one of the law enforcement officers involved in executing the warrant. (*See* Hr'g Tr., Doc. 24). Shortly after the hearing, the matter was reassigned to the undersigned judge, and the parties have completed post-hearing briefing. Due to the reassignment, the Court inquired of the parties whether a new hearing would be necessary, but both parties stated that the Court could move forward on the existing record to decide the matter.

### LAW AND ANALYSIS

The Fourth Amendment provides:

[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

As the text makes clear, “the ultimate touchstone of the Fourth Amendment is ‘reasonableness.’” *Brigham City v. Stuart*, 547 U.S. 398, 403 (2006). Generally speaking, reasonableness “requires the obtaining of a judicial warrant.” *Vernonia Sch. Dist., 47J v. Acton*, 515 U.S. 646, 653 (1995). That is because the process of obtaining a warrant means that inferences about probable cause will be “drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime.” *Riley v. California*, 573 U.S. 373, 382 (2014) (quoting *Johnson v. United States*, 333 U.S. 10, 14 (1948)).

Here, though, all agree that the government in fact obtained a warrant from a “neutral and detached magistrate,” and even agree that the warrant was supported by probable cause. (Mot., Doc. 21, #50; Opp’n, Doc. 22, #96). Bethel’s argument instead goes to the *scope* of the warrant, urging the Court to find that the warrant should have been limited to Bonavita’s cell phone, and not Bethel’s. (Mot., Doc. 21, #52).

The Court concludes that Bethel’s argument relies on a misunderstanding as to how warrants work. As a general matter, “the legality of a search [of specified premises] pursuant to a valid warrant is not suspect-specific.” *United States v. Baez*, 983 F.3d 1029, 1041 (8th Cir. 2020). So, if a warrant “authorize[s] the search of the entire premises for the items listed, officers [do] not exceed its scope by searching [one resident’s] bedroom, even though the warrant was issued based on information about activities of [another resident].” *United States v. Darr*, 661 F.3d 375, 379 (8th Cir. 2011); *see also, e.g., United States v. Ayers*, 924 F.2d 1468, 1480 (9th Cir. 1991) (“A search warrant for the entire premises of a single family residence is valid, notwithstanding the fact that it was issued based on information regarding the alleged illegal activities of one of several occupants of a residence.” (citing 2 W. LaFare, *Search and Seizure: A Treatise on the Fourth Amendment*, § 4.5(b) at 219–20 (2nd ed. 1987) and the cases cited therein)); *Matter of Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation*, 497 F. Supp. 3d 345, 361 (N.D. Ill. 2020) (“For example, when a court authorizes the search of a house, the entire house is subject to the search, and this includes the most

private areas of a house, such as bedrooms and bathrooms, of individuals who may not be involved in the crime but who nonetheless live in the premises, such as spouses and children.”). This in some ways reflects the broader principle that “a lawful search of fixed premises generally extends to every part of the premises in which the object of the search may be found, notwithstanding the fact that separate acts of opening or entry may be required to complete the search.” *United States v. Percival*, 756 F.2d 600, 612 (7th Cir. 1985); *see also United States v. Reichling*, 781 F.3d 883, 888 (7th Cir. 2015) (“Thus, a warrant that authorizes an officer to search a home for illegal weapons also provides authority to open closets, chests, drawers, and containers in which the weapon might be found.”). In other words, officers can search the entire premises, including opening any compartments or containers that are physically capable of containing the contraband for which they are searching.

To be sure, it may be suspect-specific concerns that lead to the issuance of a warrant in the first instance. That is, it may be a particular person’s routine presence at a given premises that gives rise to probable cause to search that premises. This is one aspect of what courts refer to as nexus. Stated more fully, one way in which a particular suspect’s conduct may give rise to an inference that a given location will contain evidence of criminality is if the government can show a “nexus” between the suspect and the location, such that it would be likely that the suspect stored belongings there, potentially including evidence of a crime. *See United States v. Reed*, 993 F.3d 441, 447 (6th Cir. 2021). But once that nexus is established, and the warrant issues, the suspect-specific part of the inquiry ceases. *See Baez*, 983 F.3d at 1041.

As a practical matter, that makes some sense. A suspect's presence at a location may suffice to show that evidence of that person's criminal conduct will likely be located there, with the nature of the evidence depending on the nature of the alleged crime. So, for example, if a suspected shooter resides at a given location, a warrant may issue to search the premises for a gun. But, if the location is a shared single-family premises, the items located there (i.e., a gun in the example above) are unlikely to announce who among the various residents may own them. Thus, the warrant authorizes the agents to seize all items that meet the description, independent of ownership, to assess whether the items are in fact evidence of a crime.

Any other rule could unduly crimp law enforcement's ability to search a shared, multi-person residence. After all, if the residents know that a premises search pursuant to a warrant is suspect-specific, a wrongdoer residing there (and storing evidence there) could claim that a given item belongs to another resident, and thus cannot be inspected or seized. Or the other resident, wanting to assist their housemate, could assert that on their own. And, even beyond that, the hurly-burly of executing a search warrant strikes the Court as a fraught time for officers to attempt to resolve vague or disputed claims of ownership of the various items located at the residence. Consider the situation here, where the warrant authorized a search for computers. Imagine a computer located in a common area—are officers expected to attempt to ascertain who owns that computer before undertaking a search of it? And what would be sufficient proof one way or another in the context of a search? In any event, electronics in a shared residence easily could be used by any of those who live

there. Ownership does not prevent access by others. And that is particularly true of the cell phone here, which apparently was not password protected in any way. It thus arguably constituted a container (i.e., the cell phone memory), located at the Premises, that could be storing the contraband at issue (i.e., a digital representation of the unlawful photographs)—indeed, that storage could be taking place whether Bethel knew it or not. *But see Riley*, 573 U.S. at 397 (noting that analogizing a cell phone to a container is “a bit strained,” and that the analogy “crumbles entirely when a cell phone is used to access data located elsewhere”). In short, the affidavit provided the Magistrate Judge a solid basis to believe that the router at the 36 Sioux Court address was being used to download child pornography (Bethel concedes as much), and thus the Magistrate Judge easily could have concluded (and here did) that probable cause existed to search any electronic device that was located there, and thus routinely connected to that router (meaning it could be storing such downloaded information). The cell phone at issue falls squarely within the plain language of that warrant, and thus the officers’ search of it did not violate the Fourth Amendment.

To be sure, there does appear to be at least one exception to the agents-can-search-all-items-at-the-premises rule. In *Ybarra v. Illinois*, 444 U.S. 85 (1979), police had a warrant to search a tavern. Based on that warrant, they also searched a patron who happened to be there, discovering contraband. *Id.* at 88–89. The Supreme Court held that a warrant for a premises does not give officers a right to search all persons who “happened to be [there] at the time the warrant was executed.” *Id.* at 91. “Although the search warrant, issued upon probable cause, gave the officers authority



to search the premises ..., it gave them no authority whatever to invade the constitutional protections possessed individually by the tavern’s customers.” *Id.* at 92. Based on *Ybarra*, some courts have concluded that the ability to search a residential premises does not allow officers to search guests at the residence, and that, further, a search of a guest’s items may, in some cases, amount to a personal search of the guest, requiring a separate warrant. *See, e.g., United States v. Giwa*, 831 F.2d 538, 544–45 (5th Cir. 1987). This principle extends, for example, to items that constitute an “extension” of the person, such as a purse. *See United States v. Vogl*, 7 F. App’x 810, 815 (10th Cir. 2001) (collecting cases).

But, even assuming a cell phone may constitute an extension of the person, the underlying *Ybarra* principle precluding searches of *guests* does not extend to *residents* at the premises, and thus property belonging to the latter (i.e., residents) does fall within the warrant’s scope. *See United States v. Holt*, 786 F. App’x 805, 808 (10th Cir. 2019) (noting that person who had been residing in the home for ten months “was not a mere guest,” and thus “had a connection to the premises substantial enough that his laptop fell within the warrant’s scope” in a child pornography case). Here, Bethel does not dispute that he resided at the single-family home that the warrant covered. Thus, the *Ybarra*-based exception to the general entire-premises rule does not undercut the Court’s conclusion under the Fourth Amendment here.

Moreover, even if the Court is wrong in this conclusion, and the only constitutionally proper construction of the warrant here instead is one under which the warrant does not extend to Bethel’s cell phone, the result on Bethel’s Motion

would not change. In *United States v. Leon*, 468 U.S. 897 (1984), the Supreme Court carved out what courts refer to as the good-faith exception to the exclusionary rule.

As the Sixth Circuit recently observed:

A difficult question of warrant construction makes for an easy question of *Leon* application. Under *Leon*, courts will not exclude evidence from trial that was seized “by officers reasonably relying on a warrant issued by a detached and neutral magistrate.” 468 U.S. at 913. Even if the warrant technically did not permit a search of [the defendant] and the cell phone on him, the officers reasonably could have believed it did.

*United States v. Parrish*, 942 F.3d 289, 293 (6th Cir. 2019). Just so here. Nothing on the face of the warrant would have caused a reasonable officer to believe that the warrant did not validly issue. And, given the warrant’s language, an officer reasonably could have believed that the warrant authorized a search of Bethel’s cell phone. Thus, even if the warrant could not have constitutionally authorized the search that occurred, under *Leon*, the Court still would decline to suppress the evidence located on Bethel’s phone, or the evidence that grew out of the further investigation that followed.

Bethel mounts a few different attacks on that result, but none succeed. First, noting that the Sixth Circuit has described cell phone searches as potentially raising even greater privacy concerns than residence searches, (Doc. 21, #52 (quoting *United States v. Fletcher*, 978 F.3d 1009, 1019 (6th Cir. 2020))), Bethel appears to suggest a rule under which a warrant must specifically identify each different cell phone to be searched, or at the very least separately establish probable cause as to each. (*Id.*). Bethel claims to find support for this argument in *Riley*, which he says stands for the proposition that “a search warrant is required in order to search a suspect’s phone,”

in turn tacitly supporting (or so he says) the search-warrant-specifically-identifying-each-cell-phone rule he wants the Court to adopt. (*Id.*).

That argument, though, overreads *Riley*. In *Riley*, officers had stopped the defendant for a traffic violation, which ultimately led to his arrest. *Riley*, 573 U.S. at 378. They then conducted a *warrantless* search of him pursuant to that arrest. *Id.* at 378–79. When they discovered he was carrying a cell phone, they searched it. *Id.* The Court concluded that the search was wrongful, as the officers needed a warrant to search the cell phone. *Id.* at 386.

But that holding does not lead to the result that Bethel suggests here. In this case, the officers did in fact have a warrant. And the warrant authorized a search of all computers, including cell phones, located at the address. There is no dispute that the cell phone at issue fell within that description. Thus, *Riley*'s admonition that a warrant is necessary to search a cell phone is largely irrelevant. In any event, the case lends little credence to Bethel's proposed specific-identification rule, as *Riley* had no occasion to consider the appropriateness of a warrant directed at a residence that purports to allow for search and potential seizure of all cell phones located there.

In fairness to Bethel, though, he also cites *In the Matter of Search of a Single Family Home*, No. 20 M 684, 2021 WL 3204201 (N.D. Ill. June 3, 2021), which does address that question. And it appears that the Magistrate Judge there adopted a form of individual-cell-phone-specific rule along the lines Bethel suggests here. Moreover, while Bethel does not cite to it, the district court also affirmed that decision on review, again adopting that same rule. *See* 549 F. Supp. 3d 810 (N.D. Ill. 2021).

According to those cases, the government “must have a reasonable belief that a given cell phone belongs to or is regularly used by [the suspected offender], before [the government] may seize and search the phone.” *Id.* at 815. Essentially, the rule boils down to a requirement that the government establish probable cause as to each separate cell phone it intends to search or seize at a given location, much as Bethel requests here. Moreover, the courts there grounded that rule, like Bethel seeks to do here, in a notion that cell phones “are not just another technological convenience,’ but rather microcomputers that, for many Americans, hold ‘the privacies of life.’” *Id.* (quoting *Riley*, 572 U.S. at 403).

That said, a district court opinion from another circuit is not binding precedent. And, while both opinions are thoughtful and well-written, for the reasons described above, the Court does not agree with them. In particular, as noted immediately above, these cases suggest that the warrant should be understood to extend only to cell phones that “belong[] to or [are] regularly used by” the suspected perpetrator. But, as this Court discussed above, in the shared home setting this Court cannot ascertain how officers would operationalize that rule as a practical matter. To start, residents in a shared home presumably leave their phones lying about. The fact that a given phone is, or is not, in a given room at a given time may mean little about who owns (or uses) it. Moreover, even apart from that practical problem, the residents in a shared house each presumably would have an ongoing ability to at least physically access each other’s phones (and, especially if, as here, the phone is not password protected, that physical access may well include operational access). To be sure, a

workplace may be different on both of these fronts, justifying a different rule there.<sup>1</sup> But when people share a home, there is often some level of mutual trust and close personal interaction, resulting in a greater expectation of shared use of items in the house. Perhaps then it comes down to this—the Court concludes that, in the shared home setting, a default presumption may arise that all residents will have sufficient access to other residents’ cell phones to justify a warrant directed at all such phones as a group, at least where the contraband at issue is a digital file or files that can be stored on such a device. Or, at the very least, a detached and neutral magistrate judge could conclude that a search should extend to all such phones, as the magistrate judge did here.

That last point also gives rise to another distinction between this case and the Illinois cases on which Bethel relies. There, the “detached and neutral” magistrate judge *declined* to issue the requested warrant. *Search of a Single Family Home*, 549 F. Supp. 3d at 812. If that had happened here, the Court is not saying that it necessarily would have overturned such a determination. But that is not what occurred. Rather, the magistrate judge here issued a warrant covering all computers (including cell phones) at the Premises. True, perhaps no one discussed how many people resided there as part of the application process, but nonetheless, that is the warrant that issued.

---

<sup>1</sup> Of course, workplaces also have another difference that may cut in the other direction. Namely, there is a reduced expectation of privacy in the workplace as compared to the home. *Dohner v. Neff*, 240 F. Supp. 2d 692, 703 (N.D. Ohio 2002).

And that in turn gives rise to the Court's last observation regarding the Illinois cases. Here, all agree that probable cause supported the warrant issuing. And nothing on the face of the warrant suggests that extending it to all cell phones on the Premises would violate the Fourth Amendment. Thus, even if the warrant perhaps should have been narrower, a reasonable law enforcement officer would have concluded that the warrant authorized searching Bethel's phone, meaning that, as the Court observed above, *Leon* would bar application of the exclusionary rule here, even if the Illinois cases are correct about the scope of the Fourth Amendment in general.

Beyond his proposed cell-phone-specific rule, Bethel also makes what amounts to a separate-premises argument. More specifically, he notes case law suggesting that, if officers execute a search warrant on what they believe to be a single residence, only to learn that it is in fact two or more separate residences housed under the same roof, the search warrant only applies to the residence as to which the affidavit gave probable cause. (Mot., Doc. 21, #54–55 (citing, e.g., *United States v. Shamaeizadeh*, 80 F.3d 1131, 1137–38 (6th Cir. 1996))). He then suggests that separate cell phones are akin to separate premises, meaning that a separate-premises rule requires a separate warrant for each cell phone (or at least a warrant specifying each separate cell phone, supported by probable cause as to each). (*Id.* at #55).

Again, the Court is not convinced. In the premises context, the Fourth Amendment's core concern is protecting the home from governmental intrusion absent probable cause. As the Supreme Court has explained, “when it comes to the Fourth Amendment, the home is first among equals. At the Amendment's ‘very core’

stands ‘the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.’” *Fla. v. Jardines*, 569 U.S. 1, 6 (2013) (quoting *Silverman v. United States*, 365 U.S. 505, 511 (1961)). If a single physical location comprises two or more distinct and physically separate “homes” then, it only makes sense that the government must have probable cause as to each separate home to justify intrusion.

But that reasoning does not easily extend to cell phones. To be sure, people may have privacy interests in their cell phones, even strong privacy interests, but it is a stretch to call a cell phone a home, at least as that term has historically been understood for Fourth Amendment purposes. Rather, a home is a physical location where the existence of doors and walls, coupled with the right to control access, creates a “buffer” shielding the activities of the occupants from the public (and the government) more generally. It is a place to which occupants may retreat, to use the Supreme Court’s phrasing, from public view. To be sure, people may likewise consider their cell phones, and the information stored thereon, as private, and may even use their cell phones as a means of retreat from the world around them (who has not observed people sitting and staring almost glassy-eyed at their phones?), but a cell phone is not a “home” in the same “physically private” sense that an actual home is, nor does it carry the historical imprimatur of privacy associated with more traditional understandings of that term. Thus Court declines to extend the separate-premises concept to cell phones for Fourth Amendment purposes.

But, if a cell phone is not, as Bethel suggests, a separate premises, then the question merely becomes what containers located at a particular physical address (i.e., the “home” identified in the warrant) were physically capable of holding the child pornography that the FBI had a good reason to believe was being downloaded at that physical address. As noted above, each cell phone the officers found at the Premises could fit the bill, or at least the Magistrate Judge had a reasonable basis for concluding that was the case. Each cell phone could connect to the WiFi router, and each had the ability to store digitally downloaded photographs or videos. Against that backdrop, for all the reasons noted above, the Court declines to impose on officers an obligation to attempt to sort out whose cell phone is whose at a shared residence, or which cell phones a particular resident has been “regularly using,” *see Search of a Single Family Home*, 549 F. Supp. 3d at 815, before undertaking a further investigation of a particular cell phone found at the residence to which the warrant applies.<sup>2</sup>

## CONCLUSION

For the foregoing reasons, the Court **DENIES** Bethel’s Motion to Suppress (Doc. 21).

---

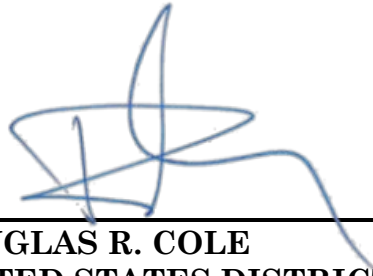
<sup>2</sup> Bethel makes one remaining argument—namely, that officers may have used his phone to access information Bethel had stored in the cloud, rather than on the phone itself. (Mot., Doc. 21, #56–57). Bethel made that argument, though, only in his opening motion. He did not elicit any testimony at the suppression hearing suggesting that had occurred, nor did he press that argument in his post-hearing briefing. Accordingly, the Court finds that Bethel has failed to prove that the officers used Bethel’s phone to access any cloud account, rendering irrelevant the question of whether the warrant would have provided officers authority to do so.



**SO ORDERED.**

August 1, 2022

**DATE**

A handwritten signature in blue ink, appearing to read 'Douglas R. Cole', is written over a horizontal line.

**DOUGLAS R. COLE**  
**UNITED STATES DISTRICT JUDGE**